#### IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF TEXAS DALLAS DIVISION

INSURANCE SAFETY CONSULTANTS, LLC and CHRISTOPHER ROBERTS,

Plaintiffs.

v.

Case No. 3:15-cv-2183-S-BT

CARRI D. NUGENT,

Defendant.

# FINDINGS, CONCLUSIONS, AND RECOMMENDATION OF THE UNITED STATES MAGISTRATE JUDGE

Before the Court in this civil action brought by Plaintiffs Insurance Safety Consultants, LLC ("ISC") and Christopher Roberts against Defendant Carri D. Nugent are two motions for summary judgment: (1) Nugent's Motion (ECF No. 148) on Plaintiffs' claims for violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), the Electronic Communications Privacy Act, 18 U.S.C. § 2510 ("ECPA"), and the Stored Communications Act, 18 U.S.C. § 2701 et. seq. ("SCA"); and (2) Plaintiff's Motion (ECF No. 151) on Nugent's counterclaim for wrongful termination under *Sabine Pilot* and for declaratory judgment. For the reasons stated, the Court should GRANT both motions, in part, and dismiss with prejudice Plaintiffs' claims under the CFAA, the ECPA, and the SCA, to the extent the claims under the ECPA and SCA related to disclosures of intercepted communications that occurred prior to June 29, 2013. The Court also should dismiss with prejudice Nugent's wrongful termination counterclaim.

#### Background<sup>1</sup>

This case arises out of a business dispute between Roberts and Roberts's former business partner, Kevin West. Roberts and West co-owned a company called Safety and Environmental Solutions, LLC ("SES"), but Roberts left SES on January 29, 2013, and started ISC. West and SES then sued Roberts and ISC in state court (the "State Court Action").

Nugent initially worked for SES. She went to work for Roberts and ISC on February 4, 2013. After ISC hired Nugent, West and SES added her as a defendant in the State Court Action and deposed her in March 2013. At a temporary injunction hearing the next month, Nugent recanted some of her deposition testimony. Also in April 2013, Roberts and ISC learned that Nugent had privileged attorney-client communications belonging to Roberts, and she had allegedly divulged Roberts's confidential information to West, SES, and their counsel in the State Court Action. *See* Def. App. 11, 16 (ECF No. 150). On April 22, 2013, Plaintiffs' counsel sent Nugent a written demand for the return of Roberts's privileged communications and confidential information. *Id.* at 26. ISC fired Nugent effective May 2, 2013; and, shortly thereafter, she went back to work for SES.

\_

Case 3:15-cv-02183-BT

<sup>&</sup>lt;sup>1</sup> Because this case is the subject of multiple prior opinions, *Ins. Safety Consultants LLC v. Nugent*, 2017 WL 735460 (N.D. Tex. Feb. 24, 2017) and *Ins. Safety Consultants LLC v. Nugent*, 2016 WL 2958929 (N.D. Tex. May 23, 2016), these Findings will recount only the background facts and procedural history necessary to understand the present recommendation.

After they fired Nugent, Plaintiffs hired a third-party vendor to investigate potential hacking by Nugent. Def. App. 41. According to Plaintiffs, the third-party vendor was ultimately unable to confirm whether any of Plaintiff's computers had been illegally accessed or whether any of their electronic communications had been illegally intercepted. Pls.' 2d Am. Compl. ¶ 30 (ECF No. 130).

On December 10, 2014, Plaintiffs deposed Nugent again in the State Court Action. During her deposition, Nugent admitted that when she set up Roberts's email service, she also configured Microsoft Outlook on her personal laptop to allow her to access Roberts's email. *See* Def. App. 83-84. Nugent further testified that, after ISC fired her, she went through Roberts's email inbox and provided copies of some of his emails to West. *Id.* at 77-78, 184-185. Based on this alleged unauthorized access, Plaintiffs filed the pending lawsuit in federal court on June 29, 2015. By their Second Amended Complaint, which is the live pleading in this case, Plaintiffs assert claims against Nugent for alleged violations of the CFAA, the ECPA, and the SCA.

Nugent answered, denying any wrongdoing, and later filed a counterclaim for wrongful termination in violation of the *Sabine Pilot* doctrine. Nugent alleges that Plaintiffs fired her in 2013 because she refused to give false testimony in the State Court Action.

Each party has moved for summary judgment as to the other's claims.

Nugent seeks summary judgment on each of Plaintiffs' claims on limitations grounds. Plaintiffs seek summary judgment on Nugent's claims on the ground

that she cannot adduce any evidence of an essential element of her *Sabine Pilot* claim. The issues have been fully briefed, and the motions are ripe for determination.

## Nugent's Motion for Summary Judgment Legal Standards

Nugent moves for summary judgment on her affirmative defense of limitations as to each of Plaintiffs' claims. Because Nugent bears the burden of proof on her limitations defense, she must establish "beyond peradventure" all of the essential elements of the defense to warrant judgment in her favor. *Fontenot v. Upjohn Co.*, 780 F.2d 1190, 1194 (5th Cir. 1986). The beyond peradventure standard imposes a heavy burden on the movant to show there are no genuine material fact disputes and that the movant is entitled to summary judgment as a matter of law. *See, e.g., Martin v. Alamo Cmty. Coll. Dist.*, 353 F.3d 409, 412 (5th Cir. 2003). On such a motion, the Court draws all reasonable inferences in favor of the nonmovant. *Chaplin v. NationsCredit Corp.*, 307 F.3d 368, 372 (5th Cir. 2002).

#### **Preliminary Matters**

Plaintiffs ask the Court to postpone ruling on Nugent's summary judgment motion and first consider their motion for sanctions (ECF No. 157), which seeks—as a remedy for alleged spoliation of evidence on Nugent's laptop—adverse inference presumptions that (1) Nugent accessed Plaintiffs' Microsoft email servers through August of 2013, and intercepted Plaintiffs' stored and "in transit"

emails during that time; and (2) Nugent disclosed the entirety of Plaintiffs emails' to SES and West. In the context of a summary judgment motion, an adverse inference presumption imposed as a sanction for spoliation of evidence may be sufficient to raise a genuine fact issue, thereby precluding summary judgment. De Los Santos v. Kroger Texas, LP, 2015 WL 3504878, at \*4 n.2 (N.D. Tex. June 3, 2015) ("If a court concludes an adverse inference instruction is warranted, then it can deny summary judgment because the adverse inference provides a genuine issue of material fact for a jury to consider.").

Plaintiffs' sanctions motion concerns ISC and Roberts's attempts to inspect Nugent's laptop computer. Plaintiffs first sought access to the laptop in February 2016. See Mot. (ECF No. 41). When Nugent refused to allow an inspection, Plaintiffs filed a motion to compel on April 12, 2016. *Id.* The magistrate judge granted the motion to compel on August 31, 2016; and, on October 6, 2016, the magistrate judge entered a written order requiring that the laptop be delivered within ten days to a neutral computer forensics investigator for examination. See Order (ECF No. 62).<sup>2</sup> Plaintiffs contend that the resulting forensic examination

[T]he Forensics Investigator will conduct a search of the laptop to locate all of Plaintiffs' emails or other documents belonging to Plaintiffs and determine when the emails or documents were obtained, in what form and in what locations they were saved, to whom they were disseminated and when. This search will include a search for all emails sent from Ms. Nugent's laptop which contain or reference Plaintiffs' emails or other documents. The Forensics Investigator is to ascertain whether any such emails or other documents were saved to other electronic devices and to identify

<sup>&</sup>lt;sup>2</sup> The Order directed:

Page 6 of 19

revealed that Nugent attempted to perform a factory reset on the laptop on September 12, 2016. See Mot. (ECF No. 157, 158). Plaintiffs further contend that, as a result of the factory reset, Nugent destroyed evidence that she accessed Plaintiffs' email accounts after June 29, 2013.

As discussed in these Findings, Plaintiffs' "belief" that Nugent illegally accessed their email accounts after June 29, 2013 is based on mere suspicion. Such suspicion is insufficient to warrant postponing consideration of the summary judgment motion. If the Court later decides sanctions are justified, the Court will still have a broad array of particular sanctions from which to choose.

#### Analysis

Plaintiffs filed this civil action against Nugent on June 29, 2015, asserting claims for violations of the CFAA, the SCA, and the ECPA. Each of these statutes has a two-year limitations period. 18 U.S.C. § 1030(g) (CFAA); 18 U.S.C. § 2520(e) (ECPA); 18 U.S.C. § 2707(f) (SCA). To prevail on summary judgment then, Nugent must show that Plaintiffs' claims accrued prior to June 29, 2013.

> any other electronic devices which were connected to Defendant's laptop computer since the interception of Plaintiffs' emails.

> The Forensics Investigator will search for evidence of document deletions or other evidence suggesting destruction of evidence. The Forensics Investigator will determine the settings used by Ms. Nugent's Microsoft Outlook to access any of Plaintiff's email. The Forensics Investigator will also search for any evidence suggesting that the laptop computer was used to access any computers or accounts of Plaintiffs, and if so, which computers or accounts, the dates of such access, and any information obtained as a result of such access.

See Order (ECF No. 67).

#### The Computer Fraud and Abuse Act

The CFAA is an anti-hacking statute that prohibits unauthorized access to protected computers for the purposes of obtaining information, causing damage, or perpetrating fraud. 18 U.S.C. § 1030(a)(2), (a)(4), (a)(5). The statute permits a plaintiff to bring a civil enforcement action "within 2 years of the date of the act complained of or the date of the discovery of the damage." 18 U.S.C. § 1030(g). "Damage," for purposes of the statute, means "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The statute of limitations thus begins to run on the date the unlawful access occurs or when unlawful access is discovered. *Higgins v. NMI Enters., Inc.*, 969 F.Supp.2d 628, 640–41 (E.D. La. 2013); *see also Quantlab Techs. Ltd. (BVI) v. Godlevsky*, 2015 WL 1651251, at \*2 (S.D. Tex. Apr. 14, 2015) ("A CFAA claim accrues as soon as the plaintiff knows of the unauthorized access[.]").

Here, Plaintiffs contend that Nugent set up email accounts for ISC and its employees, including Roberts, on January, 29, 2013, and "began intercepting Plaintiffs' emails at that time." Pls.' 2d Am. Compl. ¶ 9 (ECF No. 130). Although the alleged unauthorized access occurred outside the limitations period, Plaintiffs assert their CFAA claim is timely because they did not actually discover that Nugent had unlawfully accessed their computers until December 10, 2014, when Nugent admitted she had done so during her deposition in this case. However, the summary judgment evidence establishes that Plaintiffs discovered much earlier that Nugent had been intercepting their emails.

Among other things the summary judgment record contains a letter dated April 22, 2013, from Plaintiffs' counsel to Nugent's counsel, terminating the arrangement whereby ISC had paid Nugent's legal fees in the state court action between West and Roberts. Def. App. 2 (ECF No. 150). The letter explains, in pertinent part, that the fee arrangement was cancelled because:

It has come to our attention that your client, Carri Nugent, has improperly obtained privileged attorney client communications between me and Chris Roberts and divulged that information to Plaintiffs and/or their counsel in this lawsuit. We also have reason to believe, and do believe, that Ms. Nugent has also improperly accessed ISC's other confidential information and divulged that information to Plaintiffs and/or their counsel. Please forward me immediately all originals and copies of confidential and privileged information in Ms. Nugent's possession and please confirm that all such information has been permanently deleted from her electronic media and any hard copies not sent to me have been destroyed.

*Id.* It is undisputed that Plaintiffs terminated Nugent's employment at ISC effective May 2, 2013, after Plaintiffs learned Nugent had allegedly obtained and was making improper use of Plaintiffs' privileged communications and confidential information.

The record also contains an invoice from the third-party vendor Plaintiffs hired in May 2013 to investigate Nugent's alleged improper access to their email accounts. The invoice provides a detailed statement explaining the scope of the vendor's service, including Plaintiffs' motivation for contacting the vendor in the first place. The invoice states:

Arrived on site and spoke with Chris about their concerns.

Chris informed me that they had terminated an employee who they believed to be hacking into their systems. They mentioned "strange" occurrences of computer [sic] that were shutoff the night before being up and running the next day. Additionally they believe she had access to personal emails for Chris and other people at the firm, in addition to other personal information/accounts that she was potentially using in malicious ways.

#### Def. App. 41.

Although Plaintiffs concede they "suspected" in April and May of 2013 that Nugent hacked their computers, Plaintiffs insist they did not actually discover Nugent had accessed their emails without authorization until she testified at her December 2014 deposition and provided a detailed explanation of how she configured Plaintiffs' email accounts and the Microsoft servers to provide copies of Plaintiffs' communications to her on her personal laptop. Plaintiffs propose the April 22, 2013 letter demonstrates only that Plaintiffs believed Nugent had their confidential information—and not that Plaintiffs had specific knowledge that Nugent had illegally accessed their email accounts and the Microsoft servers on her laptop. Contrary to Plaintiffs' suggestion, however, the statute of limitations begins to run when the injured party gains awareness of an unauthorized access into its protected computers; full knowledge of all the details of the unauthorized access is not required to trigger limitations. See Higgins, 969 F. Supp. 2d at 640-41 (limitations began to run when plaintiff became aware of unauthorized access, even if he only suspected the identity of the perpetrator).

Plaintiffs further contend that their investigation into Nugent's suspected hacking and the fact that they hired a third-party vendor in May of 2013 are not sufficient to trigger the statute of limitations because the vendor did not find "evidence" of illegal access. This argument is similarly unavailing. There is no requirement that an injured party have forensic confirmation of damage under the CFAA in order for a cause of action to accrue. In *Mitchell Enters., Inc. v. Mr. Elec. Corp.*, 2014 WL 1365903, at \*4-5 (D. Idaho Apr. 7, 2014), the court rejected a similar argument that a CFAA claim did not accrue until the plaintiffs received a computer forensics report detailing the damage to their computer network, software programs, and other data. Such an argument, the court aptly explained:

would add an otherwise unexpressed layer to the [CFAA's] description of the statute of limitations—one that contemplates a more developed level of knowledge surrounding the discovery of claimed damage. . . . There is no requirement that the damage be confirmed by some sort of independent forensic examination. To add such a requirement would create a wandering line in the application of the statute of limitations, a line that would only be set if and when a party obtained such a separate or independent confirmation. That is not required to constitute the "discovery" of "damage" under the CFAA. The fact that Defendants were not exactly aware of whom or what caused the damage . . . is immaterial, when considering that such detail is unequivocally not required under the CFAA to trigger its two-year limitations period.

Id. at \*5.

Plaintiffs also point to their "belief" that Nugent continued to illegally access their Microsoft email accounts after June 29, 2013. In a declaration submitted in support of their response to Nugent's summary judgment motion,

Roberts explains that Plaintiffs' belief is based on the fact that, in the State Court Action, SES became aware that, in June and July 2013, ISC had employed the wife of a consultant whom ISC was prohibited from employing. Pls. App. 3, ¶ 4 (ECF No. 160). Roberts states "this information was not known outside of ISC and the customers at issue and was likely ascertained by Ms. Nugent continuing to have access to Plaintiffs' emails." Id. (emphasis added). Plaintiffs' assertions are wholly conclusory; Roberts fails to provide any facts to support his contention that the allegedly secret information about the consultant's wife was provided to SES by Nugent or that Nugent learned such information because she continued to have unauthorized access to Plaintiffs' computers.

The Court finds that Nugent has satisfied her summary judgment burden to show Plaintiffs had an awareness, prior to June 29, 2013, of Nugent's alleged unauthorized access to their computers and emails. This awareness prompted Plaintiffs to demand the return of allegedly improperly obtained confidential information and also prompted Plaintiffs to engage a third-party vendor to investigate the alleged hacking and restore the integrity of Plaintiffs' computer systems. The Court further finds, in view of the summary judgment record as a whole, that no reasonable trier of fact could find other than for Nugent on the issue of whether limitations has run on Plaintiffs' claim under the CFAA.

## The Electronic Communications Privacy Act &

#### The Stored Communications Act

The ECPA provides a cause of action against a person who "intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." 18 U.S.C. § 2511(1)(d); see also 18 U.S.C. § 2520(a). The SCA, in turn, provides a cause of action against any person who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system[.]" 18 U.S.C. § 2701(a)(1). Both statutes require that a cause of action "may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation." 18 U.S.C. §§ 2520(e), § 2707(f). There is no requirement under either the ECPA or the SCA that the injured party actually discover or be aware of the violation for the limitations period to begin. Brown v. Schleuter, 2010 WL 502732, at \*2 (W.D. La. Feb. 5, 2010), aff'd sub nom. Pringle v. Schleuter, 388 F. App'x 449 (5th Cir. 2010) (addressing commencement of limitations period under § 2520(e)); Sewell v. Bernardin, 795 F.3d 337, 340 (2d Cir. 2015) (addressing commencement of limitations period under § 2707(f)). Instead,

limitations is triggered if the injured person had a reasonable opportunity to discover the violation.

As discussed, the summary judgment evidence establishes that Roberts actually suspected, in early May 2013, that Nugent was hacking into ISC's email systems. Roberts suspected this because he had recently terminated Nugent, who had access to Roberts's and other ISC employees' email accounts. ISC's computers reportedly had been behaving strangely, apparently turning themselves on overnight when they had been shut down the day before. Nugent had communicated to Roberts's counsel privileged information that Roberts and his attorney shared electronically. These facts provided Roberts a reasonable opportunity to discover the violations. Indeed, the facts actually prompted Roberts to hire a third-party vendor to investigate possible hacking. *Pringle*, 388 F. App'x 449 (5th Cir. 2010) (holding limitations triggered on date plaintiff has enough notice as would lead a reasonable person to launch an investigation).

Each disclosure of intercepted information constitutes a separate violation and triggers a new limitations period. *See Fultz v. Gilliam*, 942 F.2d 396, 404 (6th Cir. 1991). In her interrogatory answers, Nugent admits that she sent emails on December 15, 2013. Pls.' App. 6-7 (ECF No. 160). Also, the date of one of the referenced emails shows that it was sent on May 12, 2014. *Id.* at 38-43. To the extent these are different documents that were not previously disclosed, Plaintiffs' ECPA claims would not be barred. The Court finds that Nugent has not established beyond peradventure that she is entitled to summary judgment on

her affirmative defense of limitations with respect to any disclosure of an email that was intercepted after June 29, 2013.

In all other respects, however, the Court finds that no reasonable trier of fact could find other than for Nugent on the issue of whether limitations has run on Plaintiffs' claim under the ECPA and the SCA.

## Plaintiffs' Motion for Summary Judgment Legal Standards

Plaintiffs move for summary judgment on Nugent's wrongful termination counterclaim—a claim for which Nugent will have the burden of proof at trial. Because Nugent will have the burden of proof, Plaintiffs' burden at the summary judgment stage is to point the Court to the absence of evidence on any essential element of Nugent's claim. See Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986). Once they do so, Nugent must go beyond her pleadings and designate specific facts demonstrating that there is a genuine issue for trial. See id. at 324; Little v. *Liquid Air Corp.*, 37 F.3d 1069, 1075 (5th Cir. 1994) (en banc) (per curiam). An issue is genuine if the evidence is such that a reasonable jury could return a verdict in Nugent's favor. See Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986). Nugent's failure to produce proof as to any essential element of the claim renders all other facts immaterial. See TruGreen Landcare, L.L.C. v. Scott, 512 F.Supp.2d 613, 623 (N.D. Tex. 2007) (Fitzwater, J.). Summary judgment is mandatory where Nugent fails to meet this burden. See Little, 37 F.3d at 1078-79.

#### **Preliminary Matters**

Nugent filed an Objection and Motion to Strike (ECF No. 155), by which she objects to Plaintiffs' use of her deposition testimony in support of their summary judgment motion because she received less than 14 days' notice of her deposition. The record establishes that counsel had been working for several weeks to set a date for Nugent's deposition. On January 25, 2017, when negotiations appeared to have stalled, Plaintiffs' counsel unilaterally noticed Nugent's deposition for February 2, 2017. Nugent promptly filed a Motion for a Protective Order, but appeared at her deposition as scheduled. After Plaintiffs filed a summary judgment motion relying, in large part, on Nugent's deposition testimony, Nugent filed a motion under Fed. R. Civ. P. 32, seeking to exclude the entire deposition and strike all references and citations to the deposition in Plaintiffs' filings. Def.'s Mot. to Strike (ECF No. 155). That is, Nugent seeks to prevent Plaintiffs from using her words against her.

Rule 32(a)(5)(A) provides: "A deposition must not be used against a party who, having received less than 14 days' notice of the deposition, promptly moved for a protective order under Rule 26(c)(1)(B) requesting that it not be taken or be taken at a different time or place—and this motion was still pending when the deposition was taken." Fed. R. Civ. P. 32(a)(5)(A). The language of this Rule provides no room for discretion; the prohibition on testimony obtained from a deposition on short notice is mandatory. *See, e.g., Automated Transactions LLC v. First Niagara Fin. Grp., Inc.*, 2011 WL 13213256, at \*1 (W.D.N.Y. May 10,

2011) (quoting *In re Settlement Facility Dow Corning Trus*t, 2010 WL 1247839, \*3 (E.D. Mich. 2010) ("The word 'must' means that the requirement is mandatory and not discretionary.")). Here, Plaintiffs scheduled Nugent's deposition on less than 14 days' notice. Nugent promptly filed a motion for a protective order, and the motion was still pending when the deposition was taken. Accordingly, Nugent's motion to strike is GRANTED, and Plaintiffs may not use Nugent's deposition testimony against her.

#### **Analysis**

#### **Sabine Pilot Claims**

Under Texas law, an employer can be liable for wrongful discharge if it terminates an employee solely for the employee's refusal to perform an illegal act. *See Sabine Pilot Serv., Inc. v. Hauck*, 687 S.W.2d 733, 734 (Tex. 1985). To prevail on a claim under this narrow exception to the at-will employment doctrine, an employee must prove that she was terminated for the sole reason that she refused to perform an illegal act. *Id.* ("[I]t is the plaintiff's burden to prove by a preponderance of the evidence that his discharge was for no reason other than his refusal to perform an illegal act."). The elements of Nugent's *prima facie* case are: "(1) she was required to commit an illegal act which carries criminal penalties; (2) she refused to engage in the illegality; (3) she was discharged; and (4) the sole reason for her discharge was her refusal to commit an unlawful act." *White v. FCI USA, Inc.*, 319 F.3d 672, 676 (5th Cir. 2003). That the Plaintiffs *required* Nugent to commit an illegal act is an essential element of the claim. Nugent cannot

prevail unless she can show Plaintiffs requested or demanded that she commit some illegal act and forced her to choose between violating the law and keeping her job. *See id.* at 676-77 (affirming grant of summary judgment against a terminated employee because the employee offered no evidence that she was required to perform an illegal act to keep her job).

Here, Plaintiffs move for summary judgment on Nugent's *Sabine Pilot* claim on the ground that Nugent cannot adduce any evidence that ISC or Roberts required her to commit perjury. In response to this argument, Plaintiff points only to her allegations, *see* Resp. 2 (ECF No. 161), which are not evidence and are not sufficient to raise a fact question as to whether ISC or Roberts required her to commit perjury. In the absence of competent summary judgment evidence sufficient to raise a fact question on an essential element of her claim, Plaintiffs are entitled to summary judgment.

Nugent's assertion that Plaintiffs lack evidence to defeat Nugent's allegations misunderstands her burden in response to Plaintiffs' summary judgment motion. Plaintiffs satisfied their summary judgment burden by pointing to the absence of evidence on an essential element of Nugent's claim—in this case, the first element of Nugent's *Sabine Pilot* claim, that Plaintiffs required Nugent to commit an illegal act. Therefore, Nugent must go beyond her pleadings and designate specific facts demonstrating that there is a genuine issue for trial on whether Plaintiffs required her to commit perjury. Nugent's failure to identify any evidence that Plaintiffs required her to give false testimony at her deposition

is fatal to her claim. Summary judgment is mandatory because Nugent has failed to meet her burden.

#### **Declaratory Judgment**

Plaintiffs also move for summary judgment on Nugent's claims for a declaratory judgment that Plaintiffs' claims are barred by limitations and the doctrine of *res judicata*. The Court's consideration of Plaintiffs' additional arguments on limitations is pretermitted by its determination that Plaintiffs' claims are barred by limitations (with the exception of Plaintiffs' ECPA claims relating to alleged disclosures after June 29, 2013), and should be dismissed with prejudice. The parties make only cursory statements regarding Nugent's *res judicata* defense and have not addressed the relevant issues with sufficient particularity to permit the Court to make a reasoned determination of whether summary judgment is appropriate. Plaintiffs are therefore not entitled to summary judgment on Nugent's claims for a declaratory judgment on *res judicata*.

#### Recommendation

The Court should GRANT Plaintiff's summary judgment motion (ECF No. 151) and DISMISS with prejudice Nugent's counterclaims for wrongful termination under *Sabine Pilot*. The Court should also GRANT in part Nugent's summary judgment motion (ECF No. 149) and DISMISS with prejudice Plaintiffs' claims for violations of the Computer Fraud and Abuse Act, as well as her claims under the Electronic Communications Privacy Act, and the Stored

Communications Act, relating to disclosures of intercepted information that occurred prior to June 29, 2013.

September 11, 2018.

REBECCA RUTHERFORD UNITED STATES MAGISTRATE JUDGE

# INSTRUCTIONS FOR SERVICE AND NOTICE OF RIGHT TO APPEAL/OBJECT

The Court directs the United States District Clerk to serve on the parties a true copy of the Findings, Conclusions, and Recommendation of the United States Magistrate Judge. Pursuant to Title 28, United States Code, Section 636(b)(1), any party who desires to object to these Findings, Conclusions, and Recommendation must serve and file written objections within 14 days after being served with a copy. A party filing objections must specifically identify those findings, conclusions, or recommendation to which objections are being made. The District Court need not consider frivolous, conclusory, or general objections. A party's failure to file such written objections to these Findings, Conclusions, and Recommendation will bar that party from a *de novo* determination by the District Court. *See Thomas v. Arn*, 474 U.S. 140, 150 (1985). Additionally, any failure to file written objections to the Findings, Conclusions, and Recommendation within 14 days after being served with a copy will bar the aggrieved party from appealing the factual findings and legal conclusions of the Magistrate Judge that are accepted by the District Court, except upon grounds of plain error. See Douglass v. United Services Auto. Ass'n, 79 F.3d 1415, 1417 (5th Cir. 1996) (en banc).